Chapter One

A NEW EPOCH—AND SPECTRUM—OF CONFLICT

John Arquilla and David Ronfeldt

Look around. No "good old-fashioned war" is in sight. There are a few possibilities—for example, on the Korean peninsula; or between China and Taiwan; or India and Pakistan; and, as usual, in the Middle East—but these do not seem imminent. Moreover, the most recent war, the Gulf War of 1990–1991, reflected the advent of the "revolution in military affairs" among U.S. forces and thus was more new- than old-fashioned—perhaps enough to discourage would-be conventional warmakers elsewhere from supposing they could win anytime soon against the newest generation of U.S. military forces. If another conventional war involving the United States occurs, it is likely to be radically different—as different from the Gulf War as it was from what had gone before, and largely for the same reason: the deepening impact of the information revolution on military affairs. And once a new war occurs, it may then be observed that the 1990s were not simply the post–Cold War period but also a new interwar period, one filled with radical change in which the contours of future conflicts were being shaped.

In this regard, the 1990s resemble the 1920s—the period after World War I. It was assumed by most political and military leaders then that major war was no longer likely. However, others worried about the possible return of major war. The worriers proved right. They were indeed living in an interwar period. It was also a time of major technological changes—with improvements in tanks, planes, and electronic warfare—leading to new doctrines that would optimize their use (e.g., *blitzkrieg*). Those who recognized that this was an interwar period thought through the conceptual problems of the day

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
1997		**00-00-1997 to 00-00-1997**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A New Epoch - And Spectrum - Of Conflict	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Graduate School of Operational and Information Sciences,Department of Defense Analysis,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
In Athena?s Camp: Preparing for Conflict in the Information Age (John Arquilla and David Ronfeldt eds.). Santa Monica, CA: RAND, 1997

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**20**	

and achieved striking successes in the opening phases of World War II—most notably, the Germans, who, in their victory in the Battle of France in 1940, achieved success in four weeks on the same ground where victory had eluded them for four years during the previous war. That is why analysts today would be well advised to be worried anew about the possibility that the present time indeed does not spell the end of major war.

When a new-fashioned war breaks out, what will it look like? On land, there may be no fronts, because fighting may occur almost anywhere anytime in a theater. The modal size of operational units of maneuver will become quite small—perhaps below the size of the typical 700-man battalion. At sea, the need for aircraft-carrier battle groups is sure to end. They will be replaced by smaller, faster, and equally capable fighting formations. The same is likely to hold for aerial warfare, which is already moving away from traditional formations, long carefully specialized in air wings of bombers and fighters. Today, the blending of the various types of aircraft in composite wings is occurring; and through stealth technology and improvements in the "information packages" of air-launched missiles, the air forces of the future will be able to do much more—with less.

Information, in all its dimensions, will enhance both the destructive and the disruptive capabilities of small units for all the services; in an information-age "battlespace," massed forces will simply form juicy targets for small, smart attackers. In the new epoch, decisive duels for the control of information flows will take the place of drawn-out battles of attrition or annihilation; the requirement to destroy will recede as the ability to disrupt is enhanced.

Despite the absence today (summer 1997) of a sizable conventional war, it takes only about one every decade or so to keep the notion high in people's minds that this is what war is really all about—the kind of war that matters most. However, for most of the world, the daily reality remains otherwise. Irregular conflicts abound; they pepper the conflict spectrum. Bands of Chechen ethnonationalists, organized more like clans than corps, have repelled the clanking, Cold War–era Russian army in bitter, murderous fighting. Hamas terrorists, disdainful of Palestine Liberation Organization (PLO) leaders, continue to hit Israeli targets. In Mexico, the Zapatista National Liberation Army (EZLN), with minimal fighting but strong protective

support from human-rights and other nongovernmental organizations (NGOs), has used novel "information operations" to put the government on the defensive, both politically and militarily. On the frontiers of violent crime, drug traffickers from Colombia and elsewhere have built huge transnational enterprises protected by paramilitary forces. Far away, high-seas pirates threaten oil-tankers and other lucrative targets, even as they expand and diversify their trade as smugglers in waters off China.

Everywhere, speculations about the kinds of conflicts that may prevail in the future emphasize these and other kinds of messy irregular conflicts that revolve around the rise of highly networked nonstate combatants and criminals, whose principal targets may, in many cases, be states. As terrorist organizations move away from traditional "great man" leadership structures (as exemplified by the PLO's Yasser Arafat) and develop diffuse, dispersed, network structures (as in the cases of Hamas and Hezbollah), they will be better able to deny culpability and may become increasingly disposed to more violent behavior. Criminal networks may become the covert arms of states aiming to pursue "strategic crime" and "criminal mercantilism," all the while denying their involvement, as some believe is likely in the case of China's involvement with the East Asian sea pirate networks.

In short, and for myriad reasons, the world is entering—indeed, it has already entered—a new epoch of conflict (and crime). This epoch will be defined not so much by whether there is more or less conflict than before, but by new dynamics and attributes of conflict. Qualitative changes will be as strong, if not stronger, than quantitative changes. The outlines of these changes have already emerged, as can be seen in the cases previously noted. These changes will involve high-tech sensors and weapons that can enable both distant standoff and close-in swarming attacks. The protagonists, and their attacks, will be more widely dispersed and more decentralized than ever before—and more surreptitious. Offense and defense will be blended. The temporal and spatial dimensions of conflict will at times be compressed, and at other times elongated. Disruption may often be the intended strategic aim rather than destruction. Nonstate actors, many of them transnational, will play roles as crucial as nation-state actors. Odd alliances may occur, notably between political and criminal and between state and nonstate actors. Often it will

not be clear who is aiding whom or fronting for whom. Traditional hierarchical actors will lose many battles as well as entire wars to newly networked actors. Notwithstanding the roles of high-tech weapons, sensors, and information and communications systems in this new epoch, less advanced technology will continue to play a role. Curious combinations of premodern and postmodern elements will appear in antagonists' ideologies, objectives, doctrines, and organizational designs.

These are just a few of the trends that are anticipated. What underlies many of them—the crucial causal and contextual dynamic—is the information revolution. How theorists and practitioners comprehend that dynamic and its effects on military affairs will guide how they seek to prepare for what may lie ahead.

RETHINKING THE DYNAMICS OF CONFLICT: CYBERWAR AND NETWAR

This book of essays about conflict in the information age shows how the information revolution is altering the nature of conflict, and why it is bringing new modes of warfare, terrorism, and crime to the fore, requiring analysts, advisers, policymakers, and folks on the front lines to rethink organization, doctrine, and strategy. While the book is admittedly a vehicle for disseminating our own writings to a broad public audience—in particular our ideas about "cyberwar" and "netwar"—the book also provides a balanced selection of some of the most insightful, instructive writings we encountered as we pondered our own notions. Indeed, many of the pieces included here were on a list of key readings about information-age conflict that circulated at high levels of the Pentagon during the end of 1996 and the beginning of 1997.

Several thematic threads run through the essays, which have been selected in part because they speak to these themes. We believe that a consensus is emerging around them (but we also know that they are not yet widely accepted and still arouse resistance in some quarters, a point to which we return in the concluding chapter).

The most basic theme is that conflicts will increasingly depend on, and revolve around, information and communications—"cyber" matters—broadly defined to include the related technological,

organizational, and ideational structures of a society. Indeed, information-age modes of conflict (and crime) will be largely about "knowledge"—about who knows what, when, where, and why, and about how secure a society, military, or other actor feels about its knowledge of itself and its adversaries.

A second theme is that the information revolution is not solely or mainly about technology; it is an organizational as well as a technological revolution. Thus, the emphasis in this volume is less on the advance of technology than on the challenges for organization—and on the interactions between technological and organizational changes that have implications for doctrine and strategy.

A third theme, which is closely related to the second, is that the information revolution favors and strengthens network forms of organization, while making life difficult for hierarchical forms. The rise of network forms of organization—particularly "all-channel networks," in which every node can communicate with every other node—is one of the single most important effects of the information revolution for all realms: political, economic, social, and military. It means that power is migrating to small, nonstate actors who can organize into sprawling networks more readily than can traditionally hierarchical nation-state actors. It means that conflicts will increasingly be waged by "networks," rather than by "hierarchies." It means that whoever masters the network form stands to gain major advantages in the new epoch. Some actors, such as various terrorists and criminals, may have little difficulty forming highly networked, largely nonhierarchical organizations; but for other actors, such as professional militaries that must continue to uphold hierarchies at their core, the challenge will be to discover how to combine hierarchical and networked designs to increase their agility and flexibility for field operations.

A fourth cross-cutting theme—reflective of the preceding three—is that the conflict spectrum is being remolded from end to end. Major alterations are looming in the nature of adversaries, in the threats they may pose, and thus in the defenses and other responses required to counter them. Information-age threats are likely to be more diffuse, dispersed, nonlinear, and multidimensional than were industrial-age threats. This will place U.S. military (and police)

forces under growing pressures to formulate new concepts for organization, doctrine, strategy, and tactics.

The fifth theme—one we impose on the volume, and that may not be fully shared by all of our colleagues here—is that two new modes of conflict in particular are going to define the information-age conflict spectrum: what we term "cyberwar" and "netwar." Both terms refer to *comprehensive* approaches to conflict based on the centrality of information—comprehensive in that they combine organizational, doctrinal, strategic, tactical, and technological innovations, for both offense and defense. Each term refers to a different end of the conflict spectrum.

Cyberwar—a comprehensive information-oriented approach to battle that may be to the information age what *blitzkrieg* was to the industrial age—will, in our view, be an ever-more-important entry at the military end of the spectrum, where the language is normally about high-intensity conflicts (HICs) and major regional conflicts (MRCs).[1] [See the end of each chapter for notes.] *Netwar*—a comprehensive information-oriented approach to social conflict—will figure increasingly at the societal end of the spectrum, where the language is normally about low-intensity conflict (LIC), operations-other-than-war (OOTW), and other, mostly nonmilitary, modes of conflict and crime. Whereas cyberwar will usually feature formal military forces pitted against each other, netwar will often involve nonstate, paramilitary, and irregular forces. Cyberwars and netwars may even be mounted at the same time, in mixes that pose uncomfortable societal dilemmas. Both concepts are consistent with the views of analysts like Van Creveld (1991) who believe that a transformation of war is under way that will lead to its increasing "irregularization." In this sense, the coming epoch of conflict will be more about Van Creveld than Von Clausewitz.[2]

At present, the U.S. military is the world's leader in thinking, planning, and preparing for the advent of cyberwar, both offensively and defensively. The United States is the only country with the array of advanced technologies (e.g., for command and control, surveillance, stealth, etc.) as well as the organizational and doctrinal flexibility to make cyberwar an attractive and feasible option. But its potential adversaries, especially nonstate adversaries, may have the lead in regard to netwar. Here, the U.S. emphasis may have to be on defensive

measures. This would continue a long trend in which the United States has prepared for waging major wars, while its adversaries may instead wage guerrilla war, terrorism, and other irregular modes of conflict. This may be partly the result of displacement—some adversaries, seeing that they should avoid or could not win at regular warfare, have opted for irregular modes, which the U.S. military may then try to treat as "lesser-included cases." Such displacement may occur again with netwar and other new, LIC-like modes of conflict and crime. But, we hope, netwar will not be perceived as a lesser-included case of information-age conflict—for it is not.

Instead of using terms like cyberwar or netwar, many analysts have treated such points under the rubric of the "revolution in military affairs" (RMA). Yet, the meat of this concept is the information revolution and its effects and implications. Early exponents viewed technological innovation as the key dynamic of the RMA. But other, recent exponents now accept that the RMA is equally, if not mainly, about organizational and doctrinal innovation—a view we have preferred since beginning our own efforts to conceptualize cyberwar and netwar. Even so, discussions about the RMA tend to focus on HICs and MRCs that revolve around regular, albeit much-modified, military forces. Exponents of the RMA have generally had less to say about the LIC (or netwar) end of the spectrum.

All these themes lead to a sixth theme that surfaces only occasionally in this book: Conflict in the information age will *not* consist primarily of "infowar" or "strategic information warfare" (SIW) or "Internetwar." In these types of conflicts, the threat is thought to reduce, one way or another, to attacks on, or by way of, computerized infrastructures for information, communications, and other crucial services. That kind of threat must be taken seriously. However, from the broad perspective of preparing comprehensively for conflict in the information age, two caveats are needed. First, while the information technology revolution is facilitating the rise of technological modes of conflict, the newest technologies may not be the only crucial factors for a cyberwar or netwar actor. Older means of communication, like human couriers and ham radios, and other mixes of old and new systems may, in some situations, do the job for the protagonist. Second, modes of conflict like cyberwar and netwar can be facilitated by, but do not necessarily depend on, "the Net" (i.e., the Internet); nor do they occur only in "cyberspace" or the "infosphere."

Some key *battles* may take place there, but a *war's* overall conduct and outcome may depend mostly on what happens in the "real world"—it will continue to be, even in the information age, generally more important than what happens in cyberspace or the infosphere. In our view, information-age modes of conflict may, or may not, involve SIW—and they may involve a lot more than SIW, especially when the protagonists are more interested in keeping the Net up than taking it down, so they can use it to mobilize their forces, disseminate their views, and try to affect the beliefs and opinions of other people.

Not everybody represented in this volume agrees entirely with our concepts of cyberwar and netwar. Some authors are not comfortable with any of the *nouveau* terms, while others would prefer different terms or phrases, like the "revolution in military affairs," or the "new way of war." Or they might define cyberwar or netwar differently from the way we do—after all, these concepts are in flux, serving the purpose of helping focus attention on the new dynamics of conflict, but are still far from being settled as to their precise definition and implications. Nonetheless, the first four themes resonate in most of the selections and help bring the authors together in what we call "Athena's camp."

NEW METAPHORS: ATHENA AND *GO*

Epochal shifts call for new metaphors. Metaphors and analogies help convey new concepts by providing simplified images that encapsulate complex points. We recommend the two following metaphors or analogies for better understanding the phenomenon of conflict in the information age.

The first is a mythological metaphor that speaks to the title of this book. Information has been associated with power, war, and the state since at least the time of the Greek gods. One ordinarily thinks of Ares, or the Roman refinement Mars, as the classical god of war. But Ares was a rather narrow, undisciplined, middle-ranking god who did not think much about what he was doing—he just stood there and fought, often rather impulsively. This is not an appropriate analogy for an epoch in which, increasingly, knowledge is fused to power. Athena, the warrior goddess of wisdom who sprung fully armed from Zeus's head and became the benevolent, ethical, patri-

otic protectress and occasionally wrathful huntress who exemplified reverence for the state, is the Greek god of war best attuned to the information age. Where warfare is about information, she is the superior deity.[3]

Athena is the only member of the Pantheon typically depicted with both sword and shield, symbols of her capabilities for both offense and defense. She could be wrathful, but unlike Ares, she took no pleasure in war and preferred to see conflicts settled peacefully, according to laws and with a sense of mercy. She was careful about bearing arms in times of peace, but when needed, she had ready access to Zeus's aegis (a unique, impenetrable body shielding) and to his devastating thunderbolt. While the owl and the olive tree were her chief symbols, she also attached to her hand-held shield the frightening head of the Gorgon Medusa, whose live gaze could turn a viewer to stone. Athena had previously instructed man in the art of confronting such terrors as the Gorgon, showing Perseus how to decapitate Medusa by using his shield as a mirror so that he could approach and combat her without making direct eye contact. Finally, one of Athena's best skills was weaving—a metaphor for network-building?

She stood for expanding the boundaries of civilization and defending them against ignorant barbarians, and, within a civilization, for pursuing intellectual enlightenment as much as material gain. One myth is particularly evocative for accepting her metaphorical relevance to the information age. According to Virgil, Troy would be powerful enough to withstand all its enemies so long as it possessed and honored the Palladium, a sacred statue of Athena provided by Zeus or Athena herself to city-states that worshipped her. Knowing this, the Greeks arranged to steal the Trojans' Palladium, spiritually denying them their access to the goddess of wisdom and war. As a result, she sided with the Greeks in the Trojan War, where she bested Ares in battle and conceived the idea, communicated to Odysseus, of the wooden "gift horse" secretly loaded with Greek soldiers. The Trojans made the epic misjudgment of hauling it inside their fortress, over the protestations of the priest Laocöon and the seer Cassandra. The rest is history, and legend.

Ever since, examining the relationship between information and power has attracted all manner of political and military theorists. In

our view, to be in "Athena's camp" is to understand that conflict—not to mention the "revolution in military affairs"—is about far more than technology; it is also about utilizing the highest levels of information—knowledge and wisdom—and about the importance of willpower and idealism in all worthy endeavors. Indeed, viewing Athena, not Mars, as the emblematic god (or goddess) of war in the information age is consistent with Clausewitz's dictum that knowledge must become capability.

More to the point, Athena corresponds, by way of her association with her namesake city-state, Athens, to the defense of democracy. To be in her camp is to uphold democracy, by viewing information (or knowledge and wisdom) as a vital dimension of a democratic society that must be protected lest it be fouled and used to weaken that society—a point to which we will return in a later discussion of "guarded openness" as a U.S. information strategy.

The second metaphor is about strategic games. In America and Europe, chess is often viewed as a metaphor for war. But, for the information age, the Oriental game of *Go* more accurately reflects the nature of conflict than does chess—Western proclivity for the game aside.

In chess, each side has a king and five other types of specialized pieces. Each piece, including the king, has a different "value" and a different ability to move. Each side lines up its pieces in assigned positions on opposite sides of the game board. Thus the two sides start by facing off along fronts separated by a "no man's land." Then, each side maneuvers in ways that are generally designed to fight for control of the board's center, to shield valuable pieces from capture, to use combinations of pieces to threaten and capture the opponent's pieces, and ultimately to achieve checkmate (decapitation) of the one-and-only king. Conventional warfare before World War II was often like this, and it has generally retained this linear flavor up through the Persian Gulf War.

The game of *Go* provides a better analogy for conflict in the information age, especially for irregular warfare and for networked types of conflict and crime at the low-intensity end of the spectrum. Whereas chess starts with all pieces on the board, *Go* begins with an empty board. It resembles a vast, grid-like chessboard with lots of tiny

squares. Each side takes turns placing pieces called “stones” anywhere on the board, one by one. But the stones are placed not in the squares as in chess, but on the points where the grid lines intersect. All stones are alike—there is no king to decapitate, and no queen or other specialization.

Once placed, a piece cannot move; it can only be removed, if surrounded and captured according to the rules. But in this game, taking pieces has secondary importance. The goal is to control more of the battlespace than one’s opponent does. Once emplaced, a piece exerts a presence in that part of the board, making it easier for the player to place additional pieces on nearby points in the process of surrounding territory. As a result, there is almost never a front line, and action may take place almost anywhere on the board at any time. The key battles are less for control of the center than of the corners and sides (since they are easier to box off). And whereas in chess no piece is ever totally secure, in *Go* a piece of territory can be made totally secure if it is surrounded in a particular way (in *Go* parlance, when the occupying pieces have two “eyes”).

Thus *Go*, in contrast to chess, is more about distributing one’s pieces than about massing them. It is more about proactive insertion and presence than about maneuver. It is more about deciding where to stand than whether to advance or retreat. It is more about developing web-like links among nearby stationary pieces than about moving specialized pieces in combined operations. It is more about creating networks of pieces than about protecting hierarchies of pieces. It is more about fighting to create secure territories than about fighting to the death of one’s pieces. Further, there is often a blurring of offense and defense—a single move may both attack and defend simultaneously. Finally, the use of massed concentrations is to be avoided, especially in the early phases of a game, as they may represent a misuse of time and later be susceptible to implosive attacks. This is quite different from chess, which is generally linear, and in which offense and defense are usually easily distinguished, and massing is a virtue. Future conflicts will likely resemble the game of *Go* more than the game of chess.

INTRODUCTION TO THE SELECTIONS

Most of the authors represented here work on U.S. government and military contracts; they have careers that depend on their ability to conduct policy-oriented research and analysis. Working in that world often involves a challenging tension. On the one hand, researchers are asked to help a particular office resolve a particular issue at a particular time—that is, to write for someone's "in-box." On the other hand, they also strive to produce studies that will engage a broad audience and have some enduring value—that is, to write with a long "shelf-life" in mind. The pieces we have selected by our contributors have each achieved such a shelf-life. They should be read by all who seek to understand the emerging nature of conflict in the information age. And they are being read by theorists and practitioners who aim to fill the next bookshelf full of studies, which will no doubt focus on preparing for conflict in the information age.

We have distributed our chapters into four parts. The first addresses the nature of the revolution in military affairs which, as our contributors note, is mostly an information-driven revolution, though one driven by more than just advanced technology. The second part builds on this theme, examining in some detail the phenomenon of "information warfare" as it may be waged in cyberspace and beyond. The third set of readings considers the societal-level implications of the information revolution, giving special attention to the rise of networked, nonstate actors. The last part provides selections that delineate the emergent paradigms that may come to displace current thinking about the context and the conduct of all forms of conflict. It concludes with a brief "look ahead," which relates our latest suggestions about how to develop an integrated view that will help to prepare conceptually, organizationally, doctrinally, and strategically for meeting and coping with all types of conflict that may emerge in the information age. However, despite these divisions, many chapters are interconnected.

Part I opens with our vision of the future spectrum of conflict, in which we propose the concepts of "cyberwar" and "netwar" and advance an argument about the imminence of radical change. The selections by Stephen Blank and Norman Davis offer careful analyses of the RMA, upholding the view that it is largely information-based and is driven as much by organizational and doctrinal change as by

technological advances. Next, Jeff Cooper urges a strategic perspective on the RMA, arguing that the new technologies, doctrines, and organizational designs must be melded together into an operating system that allows for a new way of war. Finally, we excerpt the first half of a study in which we analyze different views of information, relate them to different views of power, and draw implications for the RMA.

The present RMA is but the latest in a string of RMAs since ancient times. Historians Geoffrey Parker (1988) and Jeremy Black (1994)—who focus on the 16th and 17th centuries, respectively—elucidate the point that, RMAs evolve out of particular technological breakthroughs and organizational redesigns that, in turn, have radical effects on doctrine and strategy. There is no single cause of any RMA; all have been complex and ofttimes halting undertakings that required many years to unfold, as multiple forces played around and upon them. Most RMAs were resisted by military old-liners until the innovations proved worthwhile in battle, turning the tide against presumed odds. Some RMAs were fulfilled not by the dominant power of the period, but by rising contenders who had the motivation and the industry to try to become the next dominant power. All the selections in Part I are mainly about the future, but they reflect this historical background; and the need to proceed warily but energetically.

Indeed, if we had enlarged this volume, we would have included selections that show what theorists and strategists in other nations are thinking about information-age conflict, particularly in Russia and China, where some sharp contrasts to the American, technology-oriented approach are taking shape. Both the Russians and the Chinese are focusing on information-based concepts of strategy, doctrine, and organization—putting these at least on a par with technology, while avoiding a single-minded intent on it. In this regard, Americans may have much to learn from both the Russians and the Chinese—about concepts of nonlinearity, about military networks, and about notions that the more technologically advanced an opponent is, the more he may be vulnerable to disruptive attack. Tim Thomas (1996) points out that the Russians are well aware of their organizational and technological limitations—this is one of the reasons that their declaratory strategic policy seeks to deter information attack by threatening the possibility of Russian nuclear

retaliation. In the case of China, however, John Arquilla and Solomon Karmel (1997) point out that the Chinese have a sanguine view of the People's Liberation Army's ability to confront even the most sophisticated opponent—so long as the conflict takes place within or near the Chinese sphere of interest. Indeed, it may be that, as far as doctrines are concerned, Mao's view of "People's War" has more relevance to the information age than the U.S. Army's plans for "AirLand Battle."

With the preeminence of information in mind, the selections that form Part II examine the concept of "Information Warfare" (IW). Bruce Berkowitz provides a broad definition of IW, sketching its contours, and then focusing on important enabling factors to identify intelligence requirements for waging IW. Martin Libicki argues the case for moving away from large units of maneuver and toward a vision of "the small and the many." In addition, with a keen skeptical eye, John Rothrock asks—and answers—some key questions about the nature and attributes of IW. The authors in this part concur with the view that IW is not so much about tactical measures to disrupt an opponent's hardware, as it is about the use of information to impose one's will upon an adversary—often via cyberspace, but more often by traditional means (e.g., public diplomacy, propaganda, psychological operations, and perception management). Each author makes a number of concrete recommendations regarding the actions that need to be taken to prepare for IW, broadly defined.

But even though much of IW takes place outside of cyberspace, some IW will occur in the electronic realm. In many ways, IW in the coming years may resemble the early phases of aerial bombardment. In the 1920s and 1930s, it was noted that aircraft provided a capability to attack an enemy's home front directly—without first having to defeat his forces in the field. So, too, IW may enable a combatant to strike electronically at the information, communications, economic, and other crucial infrastructure of a society, without ever having to engage, much less defeat, its armed forces. Richard Hundley and Robert Anderson provide an insightful analysis of the types of "bad actors" that may populate this part of the conflict spectrum in the information age.[4] Hundley and Anderson also raise key questions about the desirability and feasibility of cooperation between the private sector and the government in the area of cyberspace security and safety. Part II concludes with an excerpt from a study by Robert

Anderson and Anthony Hearn in which they derive practical ideas for improving cyberspace security by drawing on their experiences with an "information wargame" based on the "Day After . . ." methodology developed at RAND by Roger Molander (see Molander, Wilson, and Riddile, *Strategic Information Warfare*, 1996).

Part III focuses on the rise of various sorts of nonstate actors, who are expected to play increasing roles in future conflicts. Criminals, terrorists, radical global activists, and others are newly enlivened by the information revolution. In our view, they are uniquely well-suited to exploit the advantages of the network form of organization. We open Part III with our assessment of how these networks may fight "netwars"—against states, sometimes in alliance with states, and finally, in some cases, simply using states as arenas for their wars with each other.

In the next selection, Brian Nichiporuk and Carl Builder ruminate about the effects of the information revolution upon society in general. They emphasize the point that improvements in computing power and interconnectivity tend to empower individuals and small groups, as opposed to nation-states, which may raise the possibility of a new form of supranational civil society—but also may pose the risk of growth in the capabilities of some very "uncivil" actors. Phil Williams explores this latter theme, noting that, in the information age, transnational criminal organizations (TCOs) are likely to exercise very significant influence in international affairs. He notes that criminal enterprises have long employed networked organizational structures, and that the information revolution may now give them the opportunity to actualize their ultimate potential. One need only consider the manner in which criminals have held Colombia hostage—using that troubled country as a hub for their transnational activities—to see that Williams's vision of the future is already being realized.

Much as the information revolution has empowered criminal networks so too will it reinvigorate terrorism, according to Bruce Hoffman. His paper presents the view that terrorists will find in advanced technology both a new set of targets and a means of controlling their own networks of dispersed actors, many of whom may or may not be acting under direct control from the professional cadres. The bombing of the World Trade Center is an example of this

"amateurization" of terror; and the rise of the Hezbollah terror network, which has no central leader, heralds the shift away from hierarchical "great man" organizations such as Yasser Arafat's PLO. Hoffman also considers the possibility that terrorists may target key nodes of their enemies' information infrastructures, with either old-style explosives or newfangled cyberspace technologies. This last point may indicate a shift to bloodless information attacks that may provoke less outrage among the target state's public, and a lower likelihood that the perpetrators will be alienated within the terrorist organization itself.

Our own concept of netwar illuminates how networked actors engage in conflict and how social netwars may take on a primarily nonviolent character. This has been the case with the war waged in Mexico since 1994 by activist NGOs to keep the government from a bloody repression of the EZLN. In Chiapas, two weeks of open fighting were followed by more than two years of negotiation and "information operations." Some of this is described in the excerpt from the article on the EZLN by David Ronfeldt and Armando Martinez. However, an ethnonationalist netwar, such as the one waged by the Chechens against Russia, may have a principally violent nature. In the Chechen case, the networking was of bands of fighters, linked by ham radios and runners, who fought and defeated the hierarchical, linear-thinking Russian Army. Thus, as we posit in the opening selection of Part III, traditional organizations have a very hard time coping with networked actors. Indeed, it will likely take networks to fight networks, much as, in an earlier era, it took tanks to fight tanks.

Lastly, Part IV focuses on some paradigms for thinking about the coming era of conflict that intend to spur specific defense planning preparations and processes. First, Richard Szafranski elucidates his concept of "neocortical warfare"—which views information-age conflict as moving extremely slowly, and as being more about fighting over knowledge than over territory or other resources. Szafranski describes the purest essence of war in the information age, suggesting that preparation may depend as much upon developing a mental discipline as on building new technological structures or engaging in the institutional redesign of hierarchical organizations. Next, we present the second half of our paper on new views of information and power, in which we exposit how these new concepts may ne-

cessitate reconfiguring American grand strategy in favor of an approach we call "guarded openness." Finally, we conclude this section, and the book, with a "look ahead" at some requirements for achieving an integrated vision of how best to prepare for conflict.

While the selections in this volume cover the six themes discussed earlier, it is not the only volume that should be perused for either introductory or advanced purposes. Two earlier insightful volumes about the future of conflict—Martin Van Creveld's *The Transformation of War* (1991) and Alvin and Heidi Toffler's *War and Anti-War* (1993)—remain timely. Valuable readings can be found in two volumes based on recent conferences at the Center for Strategic and International Studies (CSIS): *The Information Revolution and National Security,* edited by Stuart Schwartzstein (1996), and *The Information Revolution and International Security* (forthcoming from CSIS). For a military bent, see the book of readings edited by Alan Campen, Douglas Dearth, and R.T. Goodden, titled *Cyberwar* (1996) after the term we coined and James F. Dunnigan's *Digital Soldiers* (1996). In addition, the periodic journals *Comparative Strategy* and *Strategic Review* should be watched for essays on information-age conflict. Finally, an interesting array of World Wide Web pages have appeared over the last several years that provide access to a menu of readings, from official documents to critical rants—for example, take a look at these two sites and their links: http://www.stl.nps.navy.mil/c4i/ and http://www.teleport.com/~jwehling/OtherNetwars.html/

Over the past two decades, discussions and debates about the information revolution have gone through cycles of alternating enthusiasm and skepticism. Partly because of overblown expectations in recent years, more critical views are now in vogue—though not in this volume. Nonetheless, we hope that our readers will look beyond these cyclical trends in the debate. The bottom line for us and our contributors has little to do with enthusiasm or skepticism. Rather, it involves exploring these new frontiers of knowledge, trying to find out where the cutting edge is, or should be, and contributing to shaping it.

A GLIMPSE OF THINGS TO COME

If the themes that this volume emphasizes are correct, then we will be looking forward not only to new modes of conflict—and a new

spectrum of conflict—but also to new ways of preparing for and dealing with them. Some of these ways were noted in the speculations introducing this chapter: moving to smaller but highly capable units of maneuver; developing vast sensor arrays for real-time intelligence, surveillance, and target-acquisition; building capabilities for distant stand-off as well as close-in swarming attacks; etc. Perhaps the key factor—a result of the information revolution—is the increasing destructive and disruptive power of the small group or unit across the conflict spectrum. It is imperative to adapt to and innovate around this factor.

If the United States does not adjust to smaller units of maneuver, our large field armies, air wings, and naval battlegroups will be vulnerable to the attacks of nimbler foes. But if we can learn to rebuild around smaller (but stronger) military formations, the benefits may include providing for national security and military readiness at significantly reduced costs. Moreover, in light of the possibility that disruption may become more important than destruction, the potential of these small units implies that conflict in the information age may have less need of bloody battle than did warfare in previous eras. Indeed, just as the Oriental game of *Go* is replacing Western chess as the preferred game metaphor for conflict, so Sun Tzu's notions of victory with minimal violence may displace Clausewitz's emphasis on the deadly clash of armies amid fog and friction.

But it will be no easy task to accomplish such adaptation and innovation. The best that we may be able to do, at present, is to identify the key endeavors that must be undertaken to prepare for information-age conflict. As some of the selections in this volume suggest, and as we will elucidate in our concluding chapter, these preparations are bound to entail the following:

- Articulating a better understanding than we currently have of "information"—in a comprehensive sense, what it is, and is not.
- Realizing organizational and institutional redesigns along networked lines, by skillfully blending hierarchies and networks.
- Developing a new doctrine of conflict based on "swarming" that looks beyond AirLand Battle and can be applied across the full spectrum of conflict, from high to low intensity.

- Formulating an overarching strategy of "guarded openness" that will guide the wise use of economic, political, and military capabilities and resources.

These are the key challenges facing the denizens of Athena's camp.

REFERENCES

Arquilla, John, and Solomon Karmel, "Welcome to the Revolution . . . in Chinese Military Affairs," *Defense Analysis,* Fall 1997, forthcoming.

Black, Jeremy, *European Warfare, 1660–1815,* New Haven: Yale University Press, 1994.

Campen, Alan, Douglas Dearth, and R.T. Goodden (eds.), *Cyberwar: Security, Strategy and Conflict in the Information Age,* Fairfax, Va.: AFCEA International Press, 1996.

Dunn Mascetti, Manuela, *Athena: Goddess of War and Wisdom*, San Francisco: Chronicle Books, Little Wisdom Library, 1996.

Dunnigan, James F., *Digital Soldiers: The Evolution of High-Tech Weaponry and Tomorrow's Brave New Battlefield,* New York: St. Martin's Press, 1996.

Fleming, William, *Arts and Ideas*, Third Edition, New York: Holt, Rinehart, and Winston, 1968.

Graves, Robert, *The Greek Myths*, Baltimore, Md.: Penguin Books, 1960.

Hall, Lee, *Athena: A Biography*, Reading, Mass.: Addison-Wesley, 1997.

Hamilton, Edith, *Mythology*, Boston, Mass.: Little, Brown, and Company, 1969.

Molander, Roger, Peter Wilson, and Andrew Riddile, *Strategic Information Warfare,* Santa Monica: RAND, 1996.

Parker, Geoffrey, *The Military Revolution: Military Innovation and the Rise of the West*, Cambridge: Cambridge University Press, 1988.

Power, Richard, *Information Warfare*, San Francisco: Computer Security Institute, 1995.

Schwartzstein, Stuart D., ed., *The Information Revolution and National Security: Dimensions and Directions*, Washington, D.C.: Center for International and Strategic Studies, 1996.

Thomas, Tim, *Russian Views on Information-Based Warfare*, Fort Leavenworth, Kan.: Foreign Military Studies Office, 1996, http://leav-www.army.mil/fmso/

Toffler, Alvin, and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the Twenty-first Century*, Boston: Little, Brown and Company, 1993.

Van Creveld, Martin, *The Transformation of War*, New York: Free Press, 1991.

NOTES

[1]MRC is also sometimes used to refer to middle-range contingencies.

[2]The 19th century Prussian philosopher of war who, in his classic *On War*, distilled the lessons of the Napoleonic Wars, forming the basis for much of modern strategic thought.

[3]Standard sources on Greek and Roman mythology include Graves (1960) and Hamilton (1969). We also drew on Dunn Mascetti (1996) and Fleming (1968). For a darker view of Athena as being coopted by the male attraction to conflict, see Hall (1997). While Ares was refined by the Romans into Mars, Athena became Minerva. But given the Romans' penchant for specializing their gods, Minerva is mainly a goddess of wisdom, stripped of the warrior element. Thus she does not fit our purposes here.

[4]Another excellent selection about this subject is Richard Power's (1995) survey of advanced societies' many cyberspace vulnerabilities. Power also discusses the robustness against attack of these societies' infrastructures.